Emory International Law Review

Volume 26 | Issue 2

2012

From Cyber Attacks to Social Media Revolutions: Adapting Legal Frameworks to the Challenges and Opportunities of New Technology

Kristen E. Tullos

FROM CYBER ATTACKS TO SOCIAL MEDIA REVOLUTIONS: ADAPTING LEGAL FRAMEWORKS TO THE CHALLENGES AND OPPORTUNITIES OF NEW TECHNOLOGY

Kristen E. Tullos[*]

INTRODUCTION

In June 2010, a security firm in Belarus detected a new cyber worm on a client's computer in Iran.[1] As experts worked to untangle its pieces and understand its purpose, they quickly realized that the worm, called Stuxnet, was one of the most sophisticated and expensive pieces of malware ever created.[2] Over time, a consensus formed around its target: the centrifuges in Natanz, an Iranian nuclear facility.[3] While it was not the first piece of malware intended to harm industrial systems, the design was so advanced that the worm could stealthily alter its target without continued human involvement.[4] Numerous investigations have suggested that Stuxnet was a joint American–Israeli program.[5]

Although the United States has yet to officially acknowledge responsibility for Stuxnet, the National Defense Authorization Act for Fiscal Year 2012 included provisions authorizing the military to conduct offensive operations in cyberspace.[6] The United States is not alone in its acknowledgement of cyber as an offensive military tool; the fifteen countries with the largest military budgets are increasing their offensive cyber capabilities.[7] The United States has also expanded its defensive cyber capabilities, as it frequently experiences

---

[*] J.D., Emory University School of Law (2012); B.A., University of Georgia (2009).

[1] Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR, April 2011, at 152, 152, 155.

[2] *Id.* at 158.

[3] *Id.* at 159, 196.

[4] *Id.* at 158–59. Journalist Michael Joseph Gross explains it more eloquently: "Stuxnet is like a self-directed stealth drone: the first known virus that, released into the wild, can seek out a specific target, sabotage it, and hide both its existence and its effects until after the damage is done." *Id.* at 159.

[5] Ellen Nakashima & Joby Warrick, *Official Say U.S., Israel Were Behind Cyberattack on Iran*, WASH. POST, June 2, 2012, at A2.

[6] *Id.*; National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011).

[7] Editorial, *A New Kind of Warfare*, N.Y. TIMES, Sept. 10, 2012, at A24.

cyberattacks conducted by state and non-state actors.[8] According to Keith B. Alexander, Director of the National Security Agency and Commander of U.S. Cyber Command, computer attacks by criminal gangs, hackers, and other nations on American infrastructure increased seventeen-fold between 2009 and 2011.[9] Cyber is undoubtedly an important part of the military toolkit, but what legal frameworks govern its use?

Six months after the discovery of Stuxnet, a fruit vendor in Tunisia named Mohamed Bouazizi set himself on fire to protest the confiscation of his goods and harassment by local officials.[10] Like many young people, Ms. Ben Mhenni, a Tunsian blogger and activist, reported what she could find out about the incident on her blog, Facebook page, and Twitter account.[11] Despite the official media blackout, protesters used social media to rapidly disseminate information about events on the ground.[12] On January 14, the day that former President Ben Ali fled the country, people around the world were tweeting at a rate of twenty-eight tweets per second about the situation in Tunisia.[13] Despite the flurry of social media activity, Mhenni believes that "[s]ocial media didn't start the revolution. It was just a tool that helped."[14]

The Internet has drastically expanded opportunities for sharing ideas and information, while at the same time making governments, businesses, and individuals more vulnerable to harm. As new technologies become widely-available and increasingly sophisticated, the stakes only get higher. It is essential that the international community agree on a set of rules or norms to govern Internet activities. The *Emory International Law Review*'s Spring 2012 Symposium, "International Law and the Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolutions Fueled by Social Media" took on this challenge, exploring two key areas at the intersection of the Internet and international law.

On February 1, 2012, the Symposium convened scholars and practitioners to discuss how to adapt international and domestic law to the challenges

---

[8] David E. Sanger & Eric Schmitt, *Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure*, N.Y. Times, July 27, 2012, at A8.

[9] *Id.*

[10] Rania Abouzeid, *Postcard: Sidi Bouzid*, TIME, Feb. 7, 2011, at 8, 8.

[11] Kristen McTighe, *A Blogger at Arab Spring's Genesis*, N.Y. TIMES, Oct. 12, 2011, http://www.nytimes.com/2011/10/13/world/africa/a-blogger-at-arab-springs-genesis.html.

[12] *Id.*

[13] Alexia Tsotsis, *A Twitter Snapshot of the Tunisian Revolution: Over 196K Mentions of Tunisia, Reaching Over 26M Users*, TECHCRUNCH (Jan. 16, 2011), http://techcrunch.com/2011/01/16/tunisia-2/.

[14] McTighe, *supra* note 11.

presented by the Internet. Two main themes were featured in the day-long event. First, the Symposium considered how governments should respond to the changing nature of communication, particularly how it affects democratic governance and facilitates revolutionary movements. Second, it highlighted the challenges in applying jus in bello and jus ad bellum frameworks to the new landscape of cyberwarfare. Throughout the day, speakers discussing both topics considered whether existing legal frameworks are sufficient, or if a new body of law is needed to address challenges presented by the Internet.

I. DEMOCRATIZATION OF COMMUNICATION

Social media has changed the way societies organize by providing a fast and inexpensive way to transmit messages to a wide audience. Sascha Meinrath, Director of the New America Foundation's Open Technology Initiative, discussed how the Internet is empowering people to undermine local laws that they believe are wrong, thereby causing democracy itself to evolve and become more direct and participatory.[15] He advocated for greater Internet freedom to advance Article 19 of the United Nations Declaration of Human Rights, which provides that "everyone has the right to freedom of opinion and expression," including the right to "receive and impart information and ideas through any media and regardless of frontiers."[16]

Currently, the freedom to share information online is not without constraints. Providers of online content are subject to laws of the countries where they operate.[17] While there are extreme examples, such as Pakistan blocking Twitter in its entirety, other laws restrict certain content, like Germany's ban on communications denying the holocaust.[18] Websites operating in countries with severe restrictions are often faced with a difficult

---

[15] Sascha Meinrath, Dir., Open Tech. Inst., New Am. Found., Panel Discussion at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), *available at* http://youtu.be/jwO7yKFAprM.

[16] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 19, U.N. Doc. A/RES/217(III) (Dec. 10, 1948); *see also* Sascha Meinrath & Marvin Ammori, *Internet Freedom and the Role of an Informed Citizenry at the Dawn of the Information Age*, 26 EMORY INT'L L. REV. 921 (2012).

[17] Ryan Hal Budish, *Click to Change: Optimism Despite Online Activism's Unmet Expectations*, 26 EMORY INT'L L. REV. 745 (2012).

[18] *See id.* at 745; Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES, Nov. 30, 2008, § 6 (Magazine), at 50, 53.

choice: is it better to subject themselves to the regulations or protest by withdrawing from the country entirely?[19]

Ramnath Chellappa, Associate Professor at Emory University's Goizueta Business School, brought up the impact of online piracy on the music industry, as well as role of intellectual property laws in encouraging innovation.[20] It can be difficult to find the right balance of Internet freedom and regulation, and this debate came to the forefront recently in the United States following the proposal of the Stop Online Piracy Act ("SOPA") and the Protect IP Act ("PIPA").[21] After a massive opposition movement, led by large online companies like Google, Craigslist, and Wikipedia, the bills were defeated.[22] Meinrath believes that current copyright law does not comport with what people perceive as just. He characterizes the recent battles over SOPA and PIPA as the first round of many in the fight between free speech advocates and commercial interests in the United States.[23] Ryan Hal Budish, Fellow at the Berkman Center for Internet & Society, suggested that ensuring transparency should be the first step in determining what state regulation is appropriate.[24] We should understand what websites are being restricted by which countries and engage in broad dialog before reaching any normative conclusions.[25]

Control over Internet content is an important issue, especially as an increasing number of people are turning to the Internet for information.[26] The Pew Research Center reported that between 2010 and 2012, the number of Americans who viewed the news on a social media site doubled.[27] Although sites like Twitter and Facebook are not the main force underlying societal change, they do play an important role in rapidly disseminating information.

---

[19] *See* Ryan Hal Budish, Fellow, Berkman Ctr. for Internet & Soc'y, Panel Discussion at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), http://youtu.be/jwO7yKFAprM.

[20] Ramnath Chellappa, Assoc. Prof., Goizueta Bus. Sch., Panel Discussion at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), http://youtu.be/jwO7yKFAprM.

[21] Jenna Wortham, *With Twitter, Blackouts and Demonstrations, Web Flexes Its Muscle*, N.Y. TIMES, Jan. 19, 2012, at B1.

[22] *Id.*

[23] Meinrath, *supra* note 15.

[24] Budish, *supra* note 19.

[25] *Id.*

[26] *In Changing News Landscape, Even Television is Vulnerable: Trends in News Consumption: 1991–2012*, PEW RES. CTR. (Sept. 27, 2012), http://www.people-press.org/2012/09/27/in-changing-news-landscape-even-television-is-vulnerable/.

[27] *Id.*

As Meinrath put it, social media is "not the driver, but the lens through which the rest of the world can view it."[28]

Online activism is playing an important role in social movements worldwide, but it is not a substitute for traditional activism.[29] While traditional activism demands commitment and can be intimidating to outsiders; online activism usually requires less investment, and is sometimes called "armchair activism" or "slack-tivism."[30] Despite these unflattering monikers, social media has the power to influence agendas by the sheer number of people who post, comment, or blog about an issue. Budish believes that a form of activism between the two extremes should be cultivated to enhance the impact of activist movements.[31]

II. CYBERATTACKS AND INTERNATIONAL LAW

After discussing virtual activism, the Symposium participants turned to the use of cyber technology as an offensive and defense weapon. Are cyberattacks and state responses constrained by law, and if so, how? Panelists considered this question in light of three legal frameworks: jus ad bellum, jus in bello, and U.S. domestic law.

A. Jus Ad Bellum

The *jus ad bellum* framework applies to a state's decision to resort to force.[32] Two provisions of the UN Charter contain the foundation of jus ad bellum law. Article 2, paragraph 4 generally bans the "threat or use of force" against any other state.[33] Article 51 explains that a state may respond in self-defense to an "armed attack" against it.[34] As a result, a state is in violation of international law when it engages in the "use of force" without justification, such as responding in self-defense to an "armed attack" under Article 51.

---

[28] Meinrath, *supra* note 15.

[29] Budish, *supra* note 19.

[30] *Id.*

[31] *Id.*; *see also* Ryan Hal Budish, *supra* note 17.

[32] Michael Schmitt, Chairman & Prof., Int'l Law Dep't, U.S. Naval War Coll., Panel Discussion at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), http://www.youtube.com/watch?v=jDvP-z-f4tc.

[33] U.N. Charter art. 2, para. 4.

[34] U.N. Charter art. 51.

Although the drafters of the U.N. Charter were in agreement that the phrase "use of force" should not be equated with "armed attack,"[35] they did not define what constitutes a "use of force."[36] As a result, identifying a "use of force" is not always easy in the kinetic context, and only becomes more challenging when evaluating cyber activities.[37] If left unresolved, this lack of lack of clarity could lead to unpredictable and erratic state responses to cyberattacks.

In his keynote speech, Eric Greenwald, Senior Advisor to the Director of Operations at U.S. Cyber Command, pointed out that a "use of force" is clear where there is an obvious physical effect, such as the destruction of a generator.[38] The key factor in determining whether a "use of force" occurred is the effect of the cyberattack.[39] Col. Gary Brown, Staff Judge Advocate of U.S. Cyber Command, reminded the audience that information is constantly traveling through other countries, and such transit is not considered to rise to the level of a use of force.[40]

Michael Schmitt, Chairman of the International Law Department at the U.S. Naval War College, suggested a practical approach for countries to use in determining whether an action constitutes a use of force: anticipate how the international community will characterize it.[41] Certain factors can be employed, such as severity, measurability of the harm, and the invasiveness of the attack.[42]

An armed attack, which could justify action in self-defense under 51, is a higher threshold than the "use of force" under Article 2, paragraph 4. An action that rises to the level of an "armed attack" under Article 51 severely damages

---

[35] Schmitt, *supra* note 32 (noting that this interpretation was affirmed by the International Court of Justice). For a discussion of that case, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27), see *infra* text accompanying notes 87–88).

[36] *Id.*

[37] Eric Greenwald, Senior Advisor to the Dir. of Operations, U.S. Cyber Command, Keynote Speech at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), http://www.youtube.com/watch?v=jDvP-z-f4tc.

[38] *Id.*

[39] *Id.*; Catherine Lotrionte, Dir., Inst. for Law, Sci., & Global Sec., Georgetown Univ., Panel Discussion at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), http://www.youtube.com/watch?v=jDvP-z-f4tc.

[40] Col. Gary Brown, Staff Judge Advocate, U.S. Cyber Command, Panel Discussion at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), http://www.youtube.com/watch?v=jDvP-z-f4tc.

[41] Schmitt, *supra* note 32.

[42] *Id.*

property, injures people, or permanently interferes with system functionality.[43] Currently, the inquiry of whether an "armed attack" occurred also focuses on the effect of the action.[44] Lotrionte suggests working toward an international consensus on certain targets which, if targeted, would trigger the existing framework for an "armed attack."[45] One possible area of agreement might be a country's financial sector.[46] Indeed, President Obama, in a recent speech, identified national assets that must be protected against cyber incursions.[47] Redefining "armed attack" to encompass a cyberattack on crucial parts of a country's infrastructure may be one way that international law adapts to the challenges created by the Internet.[48]

Further, all uses of force in self-defense require "necessity" and "proportionality." These criteria are not contained in the UN Charter, but are instead part of customary law that international tribunals have confirmed are part of jus ad bellum law.[49] The "necessity" requirement of jus ad bellum prohibits the use of force unless a threat or attack could not be addressed through non-forcible means.[50] Responding with "proportionality" does not mean equivalent force; instead, it limits the amount of force used in self-defense to what is reasonably necessary to stop the attack or threat of attack.[51] International tribunals have yet to rule on how these requirements can be met by states responding to a cyberattack.[52] In the interim, states must use their best judgment as to whether an attack can be defended with a passive system like a firewall or if a more forcible response is needed to alleviate the threat.[53]

Practically, the use of the Internet as the delivery mechanism makes it difficult to even identity the attacker against whom you may be able to act in self-defense. Attribution is difficult in the cyber context, as the attacking entity

---

43 *Id.*

44 *Id.*

45 Lotrionte, *supra* note 39; *see also* Catherine Lotrionte, *Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825 (2012).

46 Lotrionte, *supra* note 39.

47 Eric Talbot Jensen, Assoc. Prof., Brigham Young Univ. Law Sch., Panel Discussion at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), http://www.youtube.com/watch?v=jDvP-z-f4tc; *see also* Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773 (2012).

48 *Id.*

49 Lotrionte, *Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, *supra* note 45, at 886.

50 *Id.*

51 *Id.*

52 *Id.*

53 *Id.*

can make it hard to determine who built and unleashed the malware.[54] This challenge was exemplified by Stuxnet, as it took months for a consensus to form around the idea that the United States and Israel were responsible for its creation, and, to this date, neither country has officially admitted responsibility for deploying the cyber worm.[55]

B. Jus In Bello

Jus in bello, or international humanitarian law, applies during international and non-international armed conflict to limit the harmful impact of armed conflict on humanity.[56] The jus in bello framework includes the Hague Conventions, which regulate military operations, and the Geneva Conventions, which provide protections for non-combatants, including prisoners of war and civilians.[57]

Similar to the jus ad bellum framework, it is difficult to determine if and when cyber activities trigger certain provisions, which have been previously defined, if at all, in a kinetic context. For example, when do cyber actions can constitute an "armed conflict" that triggers the protections of international humanitarian law?[58] It is unclear whether an "armed conflict" can be based solely on cyber activities.[59] Schmitt and Lotrionte recommend a focus on the effects of the cyber activity,[60] which usually requires harming people or infrastructure to rise to the level of "armed conflict."[61]

Further, it is an open question whether non-international armed conflict can be entirely virtual because it requires an organized armed group.[62] Schmitt believes that it can be entirely virtual, so long as the group's activities are well-coordinated.[63] Regardless, international humanitarian law will be difficult to apply. Because non-international armed conflicts must also rise to the level of

---

[54] Lotrionte, *supra* note 39.

[55] *See supra* text accompanying notes 1–5.

[56] INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW: ANSWERS TO YOUR QUESTIONS 14 (2004), *available at* http://www.icrc.org/eng/assets/files/other/icrc_002_0703.pdf.

[57] *Id.* at 4, 10–11.

[58] Schmitt, *supra* note 32.

[59] *Id.*

[60] *Id.*; Lotrionte, *supra* note 39.

[61] Schmitt, *supra* note 32.

[62] *Id*. Non-international armed conflict is contained within a single state. *See* INT'L COMM. OF THE RED CROSS, *supra* note 56, at 4.

[63] *See* Schmitt, *supra* note 32.

protracted conflict, it may be more feasible to apply human rights and domestic laws to cyber actions contained within a single state.[64]

Despite these challenges, existing jus in bello and jus ad bellum frameworks will likely be applied to cyber operations.[65] It is highly improbable that the international community will reach consensus on new treaty provisions to govern cyber operations.[66] As a result, several legal terms of art must be redefined so that they can be applied to this new forum for conflict.[67]

C. Domestic Law and U.S. Military Strategy

American policymakers are facing many of the same challenges integrating cyber operations into domestic policy.[68] In the National Defense Authorization Act for Fiscal Year 2012, Congress, for the first time, explicitly authorized the military to conduct offensive operations in cyberspace.[69] The relevant provisions, however, are very brief—fifty-five words to be exact:[70] Section 954 broadly authorizes cyber operations for the purpose of defending "our Nation, Allies and interests," subject to the "legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict."[71] As discussed in the previous subsections, it can be extremely difficult to apply parts of jus in bello and jus ad bellum law to cyber operations.[72]

Although Congress is trying to create a regime to govern offensive cyber operations, Greenwald expects that the eventual result will be similar to covert operations.[73] No country, including the United States, will agree to a detailed

---

64 *Id.*

65 Jensen, *Cyber Deterrence*, *supra*, note 47, at 792–823.

66 Schmitt, *supra*, note 32.

67 *See* Jensen, *Cyber Deterrence*, *supra*, note 47.

68 Greenwald, *supra* note 37.

69 National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011).

70 *Id.* The full text of section 954 reads:

> Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—(1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution (50 U.S.C. 1541 et seq.).

Id.

71 *Id.*

72 *See supra* Part II.A–B.

73 Greenwald, *supra* note 37.

governance structure because of the classified nature of the operations, as well as the fear of a double-edged sword: countries want to use cyber operations, but do not want to legitimate other countries using the same weapons against them.[74] Instead, Greenwald anticipates that there will be a push for nation–states to exercise greater control over online activity that takes place within their borders, which will make it easier to apply existing legal regimes, particularly with regard to attribution and state responsibility.[75]

In addition, U.S. military operations cannot be conducted in violation of customary international law,[76] and, therefore, cannot violate another country's sovereignty.[77] This raises an important question: How do we define a violation of sovereignty? As customary international law is developed through breach, we have to look to practice to determine its meaning in the cyber context.[78] Clearly, it is not a violation for data to travel through servers located in another country, which is different in kinetic operations where a state needs permission to intrude on another state's terrain and airspace.[79] It is hard to define at what point a digital incursion becomes a violation of sovereignty.[80] Nevertheless, the United States must work to define that threshold so as to avoid being in violation of laws that apply to the U.S. military.[81]

The U.S. military strategy of deterring cyberattacks also has to be considered in light of international law. There are many types of cyberdeterrence available to the United States, including invulnerability, invisibility, and interconnectedness.[82] An actor can also be deterred by the threat of retaliation, which can be cyber, kinetic, or legal in nature.[83] However, by signaling invulnerability, the United States could weaken its argument for necessity, which is required by international law in order to resort to use of

---

74 *Id.*

75 *Id.*

76 *Id.*

77 *See Directive No. 2311.01E: DoD Law of War Program*, U.S. DEP'T DEF. 2 (May 9, 2006), http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf (requiring the U.S. military to comply with the "Law of War," including customary international law) *cited in* 32 C.F.R. § 159.6 (2012).

78 Schmitt, *supra* note 32.

79 *Id.*

80 Brown, *supra* note 40.

81 Greenwald, *supra* note 37.

82 Jensen, *Cyber Deterrence*, supra note 47, at 806–23.

83 *Id.*

force in self-defense.[84] Lotrionte argued that the requirement of necessity applies only to anticipatory self-defense.[85]

Finally, deterrence becomes especially difficult in light of the attribution challenges created by the anonymous nature of many attacks.[86] Lotrionte and Schmitt believe that the current standard of "effective control," which the ICTY applied in *Nicaragua v. United States* to determine state responsibility,[87] will have to be loosened as a result of cyberattacks.[88] Schmitt believes it will be replaced as state practice evolves.[89] Lotrionte recommended the creation of a formal process for a state to follow in order to insulate itself from retaliation, which would include actions like admitting investigators from the state that suffered the cyberattack and making appropriate arrests.[90] Such a proposal would require a new regulatory regime, although it may be easier to generate consensus in a situation where the rules are mainly procedural in nature.

CONCLUSION

While fitting cyber operations and activities neatly into international law is a challenging task, technology has forced legal regimes to adapt throughout history.[91] Such reevaluation is apparent in areas as disparate as intellectual property and Fourth Amendment searches.[92] It is difficult to enact laws that will not require modification in light of new technology: Broad laws are hard to apply, but narrow laws quickly become outdated.[93]

Chellappa aptly framed the substantive questions at the intersection of international law and the Internet as another iteration of the age-old conflict

---

[84] Jensen, *Cyber Deterrence*, supra note 47, at 807–813; Schmitt, *supra* note 33 (citing *Caroline* case of 1837).

[85] Lotrionte, *supra* note 39.

[86] Jensen, *Cyber Deterrence*, supra note 47, at 785–87.

[87] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 65 (June 27).

[88] Lotrionte, *supra* note 39; Schmitt, *supra* note 32.

[89] Schmitt, *supra* note 32.

[90] Lotrionte, *supra* note 39.

[91] Robert Schapiro, Interim Dean, Emory Univ. Sch. of Law, Introduction at the Emory International Law Review Symposium: International Law and the Internet (Feb. 1, 2012), http://youtu.be/jwO7yKFAprM.

[92] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that use of a GPS tracking device is a search, triggering Fourth Amendment protections); Amended Verdict Form at 15, Apple Inc. v. Samsung Elecs. Co., No. 11-CV-01846-LHK (N.D. Cal. Aug. 24, 2012) (awarding nearly $1.05 billion to Apple for patent infringement claims against Samsung Electronics).

[93] *See* Budish, *supra* note 19.

between liberty and security.[94] As a society, we are constantly working to find the right balance between these two values in many different contexts. Faced with the challenges identified in the Symposium, we must strive to apply existing legal frameworks in a way that bolsters its role in education, communication, and innovation, while at the same time restricting its ability to cause harm and provoke international conflict.

[94] Chellappa, *supra* note 20.